CYBER SECURITY® INDUSTRY ALLIANCE

By Electronic Filing: Taskforcecomments@idtheft.gov

January 19, 2007

Identity Theft Task Force
Federal Trade Commission
Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Re: Identity Theft Task Force

Dear Attorney General Gonzales and Chairman Majoras:

The Cyber Security Industry Alliance (CSIA) appreciates the opportunity to comment on the efforts of the President's Identity Theft Task Force to develop a coordinated strategic plan to combat identity theft. CSIA is the only advocacy group dedicated solely to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. The organization is led by CEOs from the world's top security and technology providers, who offer the technical expertise, depth and focus to encourage a better understanding of security issues. It is the belief of the CSIA that a comprehensive approach to ensuring the security of information systems is fundamental to global protection and economic stability.

Creating a secure online environment can only be achieved through a comprehensive effort involving the implementation of appropriate public policy, effective security technology, high industry standards, and support from governments worldwide. CSIA members are united in their mission to enhance cyber security through public policy initiatives, public sector partnerships, corporate outreach, alignment behind emerging industry technology standards and public education. Because of CSIA's focus in this area, we particularly commend the work of the President's Identity Theft Task Force to address the critical need for a comprehensive plan on data security and the prevention of, not just the remedies following, identity theft.

GENERAL COMMENTS

As an initial matter, CSIA would like to note that we support comprehensive legislation on data security and breach notification that covers both the public and private sector with the same standards. A preemptive and comprehensive national law should strive to

both prevent further data breaches and address leaks when they occur. To accomplish these goals, the law must require reasonable security measures, encourage best practices such as risk assessments, access controls and encryption, create a consistent and recognizable notification standard, and include effective enforcement capabilities.

A uniform national law will simplify compliance for businesses and government. Businesses must now comply with 35 state laws, as well as federal requirements for certain industries, each with differences. Government is bound by a dizzying assortment of seemingly non-binding guidance from NIST and OMB, further to the Privacy Act and FISMA. A comprehensive law would create uniform definitions for sensitive personal information as well as a standard for the form and content of notification measures.

This is not to say that the existing federal standards should be thrown out. New legislation should not direct the creation of new standards, but draw upon existing standards set out under Gramm-Leach-Bliley, the Fair Credit Reporting Act, and industry standards that have been created in the marketplace such as the Payment Card Data Security Standard and ISO 27001. Directing the development of new standards could unnecessarily create conflicting or duplicative requirements, increasing the burden on business and increasing confusion for consumers. Rather, the new legislation should apply these tested standards to industries that are not currently bound by <u>any</u> requirements for preventative security safeguards. And the law should harmonize the government's patchwork of voluntary guidance with the definitions, triggers and mandatory safeguards applied to the private sector.

In addition, we believe preventing breaches will turn out to be less expensive than repeatedly cleaning up after them. From reports we have seen, the cost of reacting to a breach far outweighs the cost of protecting against such a breach in the first place. For instance, encrypting data so that it cannot be easily read if it falls into the wrong hands is one effective method of prevention. Encryption scrambles data in a way that makes it unreadable, except by individuals with proper keys and credentials, and thus useless to thieves and unauthorized individuals. Of course, encrypting information should include proper key management and the use of access controls to protect the keys, such as strong authentication. The cost of adequate encryption and authentication can be as little as a few dollars per customer or citizen, where the cost per person for a breach often reaches into the hundreds of dollars.

COMMENTS ON THE TASK FORCE QUESTIONS

CSIA offers the following comments for your consideration on the Task Force questions. We have not attempted to respond to all of the questions, but rather just the ones on which we have a strong opinion. Also, given the short time frame under which you must review these comments – the final report is due in less than one month – we will keep our opinions concise. We would be happy to provide a more exhaustive treatment on any item if called upon.

I. MAINTAINING SECURITY OF CONSUMER DATA

In the Task Force request for comments, the Interim Recommendations are referenced dealing with data security in the public sector. The request for comment further notes that additional measures are under consideration by the Task Force related to action in the public sector to enhance the protection of sensitive consumer information and keep it out of the hands of identity thieves. One area that stands out to us as in need of improvement on the part of the public sector is deployment of encryption technology.

While OMB guidance urging deployment of encryption technology is on the books, such as the recent guidance to encrypt mobile devices (OMB Memo 06-16, June 23, 2006), the actual funding and actual deployment of encryption throughout government agencies has been spotty at best. In particular, government agencies appear unable to receive encrypted data from companies that are required by law to regularly submit sensitive customer information.

Government agencies should deploy the technology to receive encrypted data. Many companies, particularly those in the financial services industry, are required by the government to submit sensitive personal data on their customers to government agencies such as the IRS, the Social Security Administration, the Securities and Exchange Commission and the Department of Labor. A number of the largest companies with the most consumer data encrypt their data in order to protect themselves and their customers. Yet the government agencies that require this data are unable to receive it in encrypted form. Thus the companies are forced by the government to decrypt their data, or never encrypt it in the first place, exposing sensitive consumer data to identity thieves.

I.1 and 2. GOVERNMENT AND PRIVATE SECTOR USE OF SSNs

The task force should urge the limitation on display or other inappropriate uses of social security numbers by government and the private sector, while preserving their use in authentication and business to business transactions. While not originally intended to be used as an identifier for other than social security, the number has become an integral part of many business transactions, for identification and fraud prevention. Restrictions on the use or display of social security numbers should include appropriate business to business exceptions, and should define display properly. Gratuitous use of the number, such as on badges or the outside of envelopes should be eliminated. To completely eliminate the use of the social security number for other than social security benefits would invite chaos and the need to develop a universal substitute identifier. This would entail great expense, and in the end, would bring us full cycle to a circumstance where identity thieves would seek out the new identifier with the same fervor that they now seek the social security number.

I.3. NATIONAL DATA SECURITY STANDARDS

Data security standards should apply equally to all. It is a common misconception that data breaches only affect those who shop or bank online. This is not the case. In

fact, victims span every walk of life: college students, blood donors, military personnel, hospital patients, YMCA members and customers of businesses of all sizes have all been affected.

The scope of federal data security requirements should include all entities that collect, maintain, or sell significant numbers of records containing sensitive personal information. Requirements should impact government and the private sector equally, and should include educational institutions and charitable organizations. A comprehensive response to data breach legislation is needed to ensure that information is protected at every step along the way. What could become fifty state requirements (now thirty-five), on top of overlapping federal sectoral requirements, is confusing to consumers, and both difficult and expensive for businesses to comply with.

Implementing pre-breach security measures should be central to any national security standard. An ounce of prevention is worth a pound of cure. A new federal standard should not simply require notification of consumers in case of a data breach. It should also require reasonable security measures to ensure the confidentiality and integrity of sensitive personal information in order to minimize the likelihood of a breach. Any new legislation should not direct the creation of new standards, but draw upon existing standards set out under Gramm-Leach-Bliley, the Fair Credit Reporting Act, and industry-developed standards such as the Payment Card Data Security Standard and ISO 27001. Directing the creation of new standards could unnecessarily create conflicting or duplicative standards, increasing the burden on business and increasing confusion for consumers.

Variations in standards should be based on numbers of records rather that the size of a business. CSIA is sympathetic to cost and practical concerns related to any new requirements placed on small businesses. We believe, however, that levels of security requirements should vary according to numbers of records involved and sensitivity of the data rather than size of the organization holding the data. A small organization might be in the data broker business, and should in that instance treat security as a cost of doing business. Some large organizations, on the other hand, may keep very few sensitive records and should not be forced to spend significant resources to defend non-sensitive data. A standard based on numbers and types of records would properly align incentives so as to discourage organizations and government from obtaining and keeping information that they do not need. Flexibility to existing small businesses with large numbers of records should be limited to extending transition periods for compliance.

The cost of failing to have data security far exceeds the cost of implementing a data security standard. As discussed above in our general comments, cost is a factor, but a lack of security standards is likely to be much more expensive. A recent (2006) study by the Ponemon Institute (sponsored by CSIA members PGP Corporation and Vontu, Inc) surveyed 31 companies that have experienced data breaches. The study concluded the total cost to recover from a data breach ranged from $226,000 to $22 million for the companies surveyed, representing an average total cost of $4.8 million. Companies

experienced an average total cost of $182 per lost record, a 30% increase over the 2005 study results. The cost breakdown is as follows:

- Direct incremental costs averaged $54 per lost record
- Lost productivity costs averaged $30 per lost record
- Customer opportunity costs averaged $98 per lost record

In many ways, costs to the reputations of companies are not able to be calculated. But it is clearly a cost that they would not like to have to measure. Basic security safeguards such as proper authentication, secure data storage and encryption are available comparatively on the cheap.

The cost to consumers of a data breach is significant as well. Some recent facts on the cost of identity theft include (from a 2006 Identity Fraud Survey Report from the Council of Better Business Bureaus and Javelin Strategy & Research):

- The average out-of-pocket cost for identity fraud victims is $422.
- Victims are spending more time to resolve identity fraud cases, which has increased from 33 hours per victim in 2003 to 40 hours in 2006.
- The average fraud amount per case has increased from $5,249 to $6,383, over 2 years.

I.4. BREACH NOTICE REQUIREMENTS

While the request for comments asks specifically about breach notice requirements for private sector entities, we reiterate our general theme that these standards should be applied to government based on the same standards. Half of all breaches over the last few years, and some of the largest of those breaches, have been courtesy of the public sector. Additionally, some private sector entities are already bound by breach notice requirements, such as entities subject to the federal banking regulators' guidance. As with data security requirements generally, breach notice requirements would benefit from the consistency and efficiency of one federally preempted standard.

Use of encryption or other security incentives should be a key element in establishing the threshold for breach notification. Any notification scheme should minimize "false positives." A clear reference to the "usability" of information should be considered when determining whether notification is required in case of a breach. Any new laws should include incentives such as an exemption for entities that adopt reasonable security measures or best practices when maintaining, collecting or selling consumers' personal information. Consistent with the position of consumer and financial groups, CSIA believes a provision similar to California's 1386 promoting the voluntary use of encryption as a best practice without a mandate would significantly reduce the number of "false positives," reducing the burden on consumers and business.

I.5. EDUCATION OF THE PRIVATE SECTOR AND CONSUMERS

Educating the private sector on how to safeguard data, and educating consumers in particular, is an important part of any effort to reduce identity theft. There are basic and inexpensive safeguards that even individual consumers can put in place to protect their data—everything from firewalls to anti-spyware products to encryption and more. There are basic physical steps that can be taken such as shredding sensitive account documents. A comprehensive education effort is required from government (such as through the FTC website), academia, private organizations such as CSIA and public-private partnerships such as the National Cyber Security Alliance. The President's Identity Theft Task Force is also a step in the right direction.

Support the National Cyber Security Alliance (NCSA). CSIA strongly urges the Administration to continue to support public-private partnerships such as the National Cyber Security Alliance, a 501(c)3 non-profit organization designed to educate consumers, businesses, K-12 and higher education audiences on how they can stay safe online and protect their information. The NCSA just completed a 2006 TV and Radio PSA on identify theft and how consumers and businesses can protect their information, and has a number of initiatives underway for 2007. By combining federal and corporate resources, the public and private sector can work together to solve these important issues and better educate all audiences and stakeholders.

II. PREVENTING THE MISUSE OF CONSUMER DATA

The best way to prevent misuse of data in the hands of identity thieves is to render it unreadable. Encryption and other security methods that make data unusable or unreadable to all but the most sophisticated criminals are the most logical and efficient ways to reduce the damage from a breach. As discussed above in the breach notification section, these tools should play a significant role in the "trigger" for a breach notice – properly protected data that has been lost or stolen should not require a notice. This establishes healthy incentives for holders of sensitive personal data to protect that data, while not mandating the use of particular technologies. Policy-makers should look to NIST and accepted international standards setting bodies for guidance as to what constitutes adequate security at any given time. The other benefit of the notice trigger incentive is that it avoids bombarding and desensitizing consumers with notices of data breaches that pose no significant risk of harm to them.

Authentication processes should be used. Besides rendering data unreadable, there are other effective ways to deal with a breach. One such way is to implement appropriate authentication processes that will allow an attempted user of stolen data to be recognized. Authentication should also be part of any data security program prior to a breach, thereby lowering the likelihood of an unauthorized user gaining access to sensitive data.

CONCLUSION

CSIA commends the Task Force for undertaking this effort. With the upcoming federal legislative season presenting the possibility of a dozen committees, spanning both sides of the Capitol and every industry, calling upon Administration representatives to present their views on data security, a well considered policy position is in order. We urge the Task Force to consider our three main principles as they develop a consolidated position: 1) data security and breach notice requirements should apply equally to all who hold sensitive data including government; 2) implementing pre-breach security measures should be central to any proposal; and 3) a risk-based approach to breach notice should be adopted that incentivises the use of encryption and other security methods.

Thank you for considering the views of the Cyber Security Industry Alliance.

Sincerely,

Liz Gasster
Acting Executive Director and General Counsel
Cyber Security Industry Alliance
2020 14th St. N., Suite 750
Arlington, VA 22201

lgasster@csialliance.org